

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

SOCIÉTÉ DU FIGARO, SAS, *et al.*,

Plaintiffs,

v.

APPLE INC.,

Defendant.

No. 4:22-cv-04437-YGR (TSH)

JOINT LETTER BRIEF REGARDING PROTECTIVE ORDER

The Honorable Thomas S. Hixson
San Francisco Courthouse
Courtroom B, 15th Floor
450 Golden Gate Avenue
San Francisco, CA 94102

Dear Judge Hixson:

Pursuant to the Court's Discovery Standing Order, plaintiffs Société du Figaro, SAS; L'Équipe 24/24 SAS; and le GESTE (Plaintiffs) and defendant Apple Inc. (Apple) respectfully submit this joint letter brief regarding the form and substance of the protective order to be entered in the above-referenced matter.

Counsel for the parties attest that they have met and conferred telephonically in good faith efforts to resolve this matter. Unfortunately, they have been unable to reach agreement; hence, the need for this joint letter and the Court's assistance.

DATED: December 23, 2022

HAGENS BERMAN SOBOL SHAPIRO LLP

GIBSON DUNN CRUTCHER LLP

By: /s/ Steve W. Berman
Steve W. Berman
*Counsel for Plaintiffs and the
Proposed Classes*

By: /s/ Caeli A. Higney
Caeli A. Higney
Counsel for Apple Inc.

Joint Discovery Letter Brief
December 23, 2022

Plaintiffs’ position and final proposed compromise: Plaintiffs respectfully ask the Court to enter their proposed protective order, which is attached as Ex. A. Plaintiffs sent it to Apple on December 13, 2022, as their final proposed compromise. Alternatively, Plaintiffs ask the Court to order that the parties are subject to terms of the stipulated amended protective order (ECF No. 381) from the related case *In re Apple iPhone Antitrust Litig.*, N.D. Cal. No. 4:11-cv-06714-YGR. (Ex. B.) Plaintiffs also ask the Court to reject the Apple-proposed terms discussed below.

Background: France-based iOS developers, and an association representing certain France-resident iOS developers, filed this case on August 1, 2022. (ECF No. 1.) Among other claims, Plaintiffs allege that Apple has willfully acquired and maintained monopoly (or, alternatively, monopsony) power as it relates to iOS app distribution and in-app payment (IAP) services. (ECF No. 48.) Plaintiffs also allege that Apple has overcharged France-resident iOS developers for distribution and IAP services (or underpaid them for their digital products).

The Court related this matter to *In re Apple iPhone Antitrust Litig.* (brought by App Store consumers) and to *Epic Games, Inc. v. Apple Inc.*, N.D. Cal. No. 4:20-cv-5640-YGR, on September 2, 2022. (ECF No. 28.) As the Court may recall, *Cameron v. Apple Inc.*, N.D. Cal. No. 4:19-cv-03074-YGR, a U.S.-resident iOS developer case in which the parties were represented by the same counsel as in the instant matter, also was related to *In re Apple iPhone* and *Epic Games*, but *Cameron* has settled. In this case, Apple has agreed to make available to Plaintiffs all discovery materials it made available to the consumer, *Cameron*, and *Epic Games* plaintiffs in their cases, but not until a protective order has been entered here.

On October 24, 2022, Plaintiffs sent a draft protective order to Apple for its consideration. Plaintiffs based this draft on the amended protective order still in place in the *In re Apple iPhone* consumer matter, which order was founded on the Court’s model form for cases involving highly sensitive confidential information. This should have been without controversy. Apple previously had negotiated, and agreed to, the terms of the consumer (and *Cameron*) protective order, and Plaintiffs’ draft contained only minor variations to reflect facts of the instant case. But Apple was not satisfied; it wanted more. And so, since the end of October, the parties have engaged in multiple meet-and-confers. Throughout, Plaintiffs have considered Apple’s proposed new terms in good faith and have agreed to some, which terms are reflected in the draft Plaintiffs sent to Apple on December 13. Apple, however, rejected Plaintiffs’ compromise and responded with its December 19 draft. Thus, despite Plaintiffs’ efforts to narrow the issues, the parties are at an impasse. Apple’s December 19 proposal still contains unnecessary and unwarranted additional terms, as well as an entirely new section consisting of novel, elaborate, and unjustifiable “data security provisions,” to which Plaintiffs cannot consent. Plaintiffs address each of these below.

Argument: Courts in this judicial district have routinely noted that the “model protective order is presumptively reasonable.” *See, e.g., In re Lithium Ion Batteries Antitrust Litig.*, 2017 WL 930317, at *3 (N.D. Cal. Mar. 9, 2017) (citing *Karl Storz Endoscopy-Am., Inc. v. Stryker Corp.*, 2014 WL 6629431, at *2 (N.D. Cal. Nov. 21, 2014)); *cf.* Discovery Standing Order for Magistrate Judge Thomas S. Hixson (Sept. 15, 2021) (“If parties believe a protective order is necessary, they shall, where practicable, use one of the model stipulated protective orders. . . .”). Nonetheless, Plaintiffs in related matters previously accommodated Apple’s requests for variations. The resulting protective order, still in place in *In re Apple iPhone*, has served the litigants well.

Joint Discovery Letter Brief
December 23, 2022

But Apple seeks yet more material deviations to the model order, despite no justification grounded on the facts of this case. Simply put, Apple has not met, and cannot meet, its burden of demonstrating that “*specific harm and prejudice . . . will result* if its request is not granted.” *ESC-Toy Ltd. v. Sony Interactive Ent. LLC*, 2022 WL 1714627, at *2 (N.D. Cal. May 27, 2022) (emphasis added) (internal citations omitted); *accord*, *Corley v. Google, Inc.*, 2016 WL 3421402, at *1 (N.D. Cal. June 22, 2016). Consequently, there is no basis for allowing any further deviation from the model order. *Cf. Best v. Smith*, 2020 WL 6700444, at *1 (N.D. Cal. Nov. 13, 2020) (Judge Gonzalez Rogers noting that “the Court routinely enters the model stipulated protective order for standard litigation,” and rejecting “extraneous paragraphs to the model order” that were “not warranted in this instance”). As for the terms at issue:

Treatment of non-protected material as if it were Protected Material (Sec. 7.1): As modified, Sec. 7.1 of Apple’s draft would treat all ordinary, non-confidential produced in discovery as if it were Protected Material. This is beyond the scope of a protective order as contemplated by Fed. R. Civ. P. 26(c) (referring to protection from “annoyance, embarrassment, oppression, or undue burden or expense”). This proposed term goes too far for no good reason, particularly with no showing of any actual grounds for such relief. Respectfully, it should be rejected.

“Data security” provisions (Sec. 9): In this novel proposed section (Apple cites to six *agreed* or *stipulated* protective orders, only three of which are from N.D. Cal. cases, with one of those an *agreed* order in *Apple Inc. v. Rivos* allegedly involving “gigabytes of sensitive SoC specifications and design files”), Apple seeks to impose so-called “data security” duties on Plaintiffs that are vague (*see, e.g.*, Sec. 9.5, referring broadly to “Applicable Data Law”), elaborate, and unduly burdensome. Indeed, the pertinent sections of Apple’s cited protective orders and its Sedona Conf. sample (concerned, per the commentary at viii, with “certain classes of information (*e.g.*, personal information) because of international and domestic Data Protection Laws”) bear little resemblance to proposed Sec. 9. For example, where addressed as such, all but its *agreed Rivos* protective order say it is enough if a party’s *vendor* (as distinct from a party) has an “information-management system” in place. And in fact, as Plaintiffs have advised Apple, the document-database vendor they have selected—the same one that consumers use in their related case, whose selection by Plaintiffs will spare Apple from having to transmit documents separately to them—already complies with at least one security standard referenced by Apple in its proposed Sec. 9.1, among other standards. Also, of course, Plaintiffs’ counsel have their own security measures in place. What’s more, Apple’s proposed duties would become effective on mere suspicion of breaches to storage devices, Sec. 9.2, even if Plaintiffs or their vendors have no knowledge that any of Apple’s Protected Material has been, or potentially has been, affected in any way (unlike the agreed terms in *Rivos*). In short, the specifics of proposed Section 9, including its vague requirement that Plaintiffs “implement an information security management system” periodically reviewable on 10 business days’ notice, Sec. 9.1, together with another (non-*Rivos*) requirement that they subject themselves to discovery in the event of a possible data breach, Sec. 9.4—again without actual knowledge or belief that Apple Protected Material was involved—are unfair, unworkable, and unjustified overreach. Apple in no way meets its burden to show that it will suffer specific harm if these patently unreasonable terms are not imposed, and Plaintiffs ask that its proposed new Sec. 9 be rejected.

Compulsory disclosure of information regarding so-called “Data Breaches” (Sec. 10): Apple seeks to impose notification and cooperation duties on Plaintiffs if a subpoena or court order were

Joint Discovery Letter Brief
December 23, 2022

to issue in other litigation as to “information concerning an actual or suspected Data Breach *possibly* involving a Designating Party’s Protected Materials.” (Emphasis added.) Apple would impose these duties on mere suspicion and possibility that its Protected Materials merely *might* be involved. This proposed term is unnecessary and unworkable, and Apple has not demonstrated that it will suffer specific harm if it is not imposed. It should be rejected.

Non-waiver as to manually reviewed material (Sec. 13.1): Apple proposes to extend a negotiated term in the agreed *In re Apple iPhone* protective order regarding privileged or protected documents that a party claims to have been inadvertently produced. Currently, the term provides that purportedly inadvertent production of purportedly privileged or protected materials “without manual review . . . is not and shall not be deemed a waiver or impairment of any claim of privilege or protection” Apple’s revised term would grant the same status even to material that *was* manually reviewed before production. However, if a party purports to have inadvertently produced privileged or protected materials despite manual review, that party can and should follow available procedures to determine whether in fact there is waiver or impairment. *See, e.g.*, Fed. R. Civ. P. 26(b)(5)(B). Apple can point to no specific harm that will occur if it does not receive this over-generous revision; thus, the term should be rejected.

Redundant provision regarding destruction of materials (Sec. 15): The parties’ obligations on final disposition are ample to ensure that vendors return or destroy litigation materials. Further, Apple’s proposed deviation would require certification from a party on behalf of its vendor, even though the party has no direct access to all that vendor’s systems. Apple has not indicated how denying this request will result in specific harm to it. Therefore, the proposed insertion should be rejected.

Joint Discovery Letter Brief
December 23, 2022

Apple's position: Apple respectfully asks this Court to enter its proposed protective order (Ex. C), including the following provisions: (1) reasonable data-security protections for electronic discovery; (2) making clear that discovery produced for use in this case is not to be used outside the litigation; (3) that inadvertent-production provisions apply to all documents; and (4) that return-or-destroy provisions apply to material held by vendors.

Data Security Protections Are Necessary In Light of Growing Cybersecurity Threats.

Organized criminal groups and hostile state actors are perpetrating data security breaches with growing frequency, and law firms and their vendors have increasingly become targets of these attacks. The number of security breaches increased by 17% in 2021, and of all ransomware attacks in the first quarter of 2021, 24.9% targeted small and medium sized law firms.¹ In light of this real and mounting threat, protective orders must be updated with adequate measures for handling electronic documents and data and responding to an actual or suspected data breach.² These provisions are overdue. In 2017, recognizing this rapidly changing landscape, the Sedona Conference recommended that protective orders include detailed data-security provisions.³ The risks related to data transferred and held for discovery purposes have only increased since then, leading multiple federal district courts to approve protective orders including such provisions.⁴

Here, Apple proposes that the parties and their vendors implement at least one recognized cybersecurity framework, such as the Critical Security Controls published by the Center for Internet Security (CIS). Ex. C, § 9.1. In a 2016 “California Data Breach Report” signed by then-Attorney General Kamala Harris, the California Department of Justice identified those CIS Controls as providing “a minimum level of information security that all organizations that collect or maintain personal information should meet.”⁵ As Plaintiffs indicate that their professional vendor already complies with one of the proposed frameworks, any alleged burden imposed by this provision is minimal. To prevent unauthorized access, Apple also proposes that the parties encrypt protected materials in transit⁶ (and at rest, where reasonably practical) and implement multi-factor authentication (MFA) for access, a simple measure that has been called “the single

¹ *Why Cybersecurity Should Be Top of Mind in 2022*, JDSupra (Jan. 27, 2022), [tinyurl.com/mtsfz284](https://www.tinyurl.com/mtsfz284); Xiumei Dong, *Amid BigLaw Data Attacks, Breaches Surge For Smaller Firms*, Law360 (June 15, 2022), [tinyurl.com/899wzdwz](https://www.tinyurl.com/899wzdwz); see also *Uber Verdict Raises New Risks for Ransom Payments*, Coveware (Oct. 26, 2022), [tinyurl.com/mpxbdtuy](https://www.tinyurl.com/mpxbdtuy).

² Robert Hilson, *Why the archaic process of eDiscovery is vulnerable to hacking and data breach*, Logikcull (Feb. 8, 2017), [tinyurl.com/mprnbvpz](https://www.tinyurl.com/mprnbvpz); *Data Breach Investigations Report*, Verizon (2022), [verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf](https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf).

³ *Sedona Conference International Principles: Discovery, Disclosure & Data Protection In Civil Litigation*, Sedona Conference, at vi, 53-54 (Transitional ed. Jan. 2017), [tinyurl.com/y25ehr67](https://www.tinyurl.com/y25ehr67).

⁴ See, e.g., *Apple Inc., v. Rivos, Inc.*, Case No. 5:22-cv-2637, (N.D. Cal. Oct. 31, 2022) (Dkt. 113, § 8); *Sheet Metal Workers' Nat'l Pension Fund v. Bayer Aktiengesellschaft*, Case No. 3:20-cv-04737-RS (N.D. Cal. Oct. 6, 2022) (Dkt. 138, § 7.6); *Anderson v. Gen. Motors, LLC*, Case No.: 2:22-cv-00353-KJM-DMC (E.D. Cal. Sept. 6, 2022) (Dkt. 38, § 29); *K-fee Sys. GmbH v. Nespresso USA, Inc.*, 2:21-cv-3402-GW (C.D. Cal. Apr. 28, 2022) (Dkt. 159, § 32); *Teradata Corp. v. SAP SE*, Case No. 3:18-cv-03670-WHO (N.D. Cal. May 14, 2019) (Dkt. 98, § 15).

⁵ *California Data Breach Report*, Cal. Dep't of J., at v (Feb. 2016), [tinyurl.com/3f743cd7](https://www.tinyurl.com/3f743cd7).

⁶ See *Data Protection: Data In transit vs. Data At Rest*, DataInsider (Digital Guardian's Blog) (Nov. 28, 2022), [tinyurl.com/t9kjt27](https://www.tinyurl.com/t9kjt27).

Joint Discovery Letter Brief
December 23, 2022

most important thing Americans can do to stay safe online.”⁷ *Id.* § 9.1. A party could satisfy this MFA requirement by registering users’ computers as trusted devices, after which they can access protected materials with a password—a process commonly used across corporate America today.⁸ To ensure that responsive action can be taken immediately in the event of an actual or suspected data breach, Apple proposes that the party incurring a breach notify the other party within 48 hours.⁹ *Id.* § 9.2. Apple’s proposal also provides for the parties’ cooperation following a breach, so as to help effectively and expeditiously terminate and prevent unauthorized access. *Id.* §§ 9.3-9.4. Similarly, given the likely sensitivity around the fact that a producing party’s confidential material was affected in a data breach, the parties should notify and cooperate with each other when information about a breach may be produced in other litigation. *Id.* § 10. Apple proposes that the party incurring a breach submit to reasonable discovery concerning the breach, permitting the parties to understand the related circumstances.¹⁰ These provisions set clear expectations on basic steps for investigation after a breach. None of these provisions imposes significant burden on the parties, but taken together, they provide strong protections from real and serious dangers.

Apple goes to great lengths to protect its customers’ personal data, its partners’ business information shared in confidence, and Apple’s own trade secrets and other sensitive information. *See, e.g., Epic Games, Inc. v. Apple Inc.*, 559 F. Supp. 3d 898, 949 (N.D. Cal. 2021). In this matter, Apple has already agreed to produce (and may be required to produce more) sensitive data—such as financial projections that could move markets, emails among Apple’s top executives, and transactional data reflecting (anonymized) app download histories of iPhone user accounts. That data should be safeguarded with *at least* minimum data security standards, as Apple proposes.

Plaintiffs’ refusal to stipulate to these reasonable minimum standards is without merit. Plaintiffs point to the lack of known data-security breaches affecting discovery in the related App Store actions. But good fortune in previous cases does not at all guarantee that the language in the protective orders entered there—without specific data-security requirements—suffices to guard against future attacks. This is especially true in light of the mounting cybersecurity attacks on law firms and their vendors in at least the last two years. Malicious online actors have become only savvier, and they have increasingly recognized the wealth of sensitive data exchanged in litigation. Plaintiffs’ argument that it has not happened to them yet does not provide comfort to Apple and should not provide comfort to this Court. Plaintiffs also suggest that Apple’s proposed provisions are vague—but it is Apple that seeks to set clear expectations regarding data security using terms of art such as “information security management system,” defined in the proposed frameworks. Should Plaintiffs wish to propose even more definite language, they are free to do so.

The time for updated protective-order provisions reflecting the current threat environment is now—not after a future attack. Contrary to Plaintiffs’ framing, Apple does not seek to implement

⁷ Jen Easterly, *Next Level MFA: FIDO Authentication*, Cybersecurity & Infrastructure Security Agency (Oct. 18, 2022), tinyurl.com/bdenbcxp; *see also* D. Howard Kass, *CISA Director Jen Easterly Issues Call to Action for Multi-factor Authentication, Passwordless Security*, MSSP Alert (Oct. 20, 2022), tinyurl.com/4hd4thyh; *see also, e.g.*, 16 C.F.R. § 314.4.

⁸ *See, e.g., Eric Griffith, Multi-Factor Authentication: Who Has It and How to Set It Up*, PCMag (Jan. 19, 2022), tinyurl.com/ez86rmt2.

⁹ *See also CIS Critical Security Control 17: Incident Response and Management*, CIS, tinyurl.com/ycy8a3bv (“Establish a program to develop and maintain an incident response capability . . . to prepare, detect, and quickly respond to an attack.”).

¹⁰ *See Sedona Conference, supra* n.3, at 54.

Joint Discovery Letter Brief
December 23, 2022

unilateral obligations or to gain any litigation advantage. The proposed provisions are mutually applicable, reasonable, and appropriate to manage the risk to data produced by all parties.

No Discovery Materials Should Be Used Outside the Litigation. Materials produced in discovery are produced for use in the case at issue, not for other purposes. For example, even if deposition testimony is not designated confidential or highly confidential, a law firm should not be allowed to use deposition video in its advertising or CLE presentations. Accordingly, Apple proposes language that departs slightly from the model protective order to protect against this kind of risk.¹¹ Ex. C, § 7.1. Apple does *not* seek to treat all discovery material as if it were protected. Again, Plaintiffs do not justify their refusal to stipulate to this provision.

All Inadvertently Produced Material Should Receive the Same Protections. Apple proposes that production of privileged or otherwise protected documents would not waive such protection. Ex. C, § 13.1. This is consistent with the treatment that Plaintiffs agree to for materials not manually reviewed—and they give no reason for treating other materials inconsistently. Without these provisions, Apple agrees that discovery would be entitled to protections under the Federal Rules of Civil Procedure, as well as the Federal Rules of Evidence.

The Requirements to Return or Destroy Protected Material Should Apply to Vendors. Apple’s proposal that return-or-destroy provisions apply to material held by both a party and its professional vendor adds clarity to these requirements. Ex. C, § 15. Plaintiffs argue that this requirement with respect to vendors need not be committed to writing; instead, they simply say, “trust us.” But as discussed above, Apple seeks reasonable protections, not merely Plaintiffs’ assurances that they will protect Apple’s confidential information.

¹¹ See, e.g., *SS&C Techs. Holdings, Inc. v. Arcsesium LLC*, Case No. 22-cv-2009, § 4.1 (S.D.N.Y. May 5, 2022) (Dkt. 29).